

Groups with fractionally exponential subgroup growth

Dan Segal

All Souls College, Oxford OX1 4AL, United Kingdom

Aner Shalev

Institute of Mathematics, The Hebrew University, Jerusalem 91904, Israel

Communicated by P.H. Kropholler

Received 15 December 1992

To Karl Gruenberg, whose youthful enthusiasm
continues to be an inspiration

Abstract

Segal, D. and A. Shalev, Groups with fractionally exponential subgroup growth, *Journal of Pure and Applied Algebra* 88 (1993) 205–223.

We prove that, if the subgroup growth of a finitely generated metabelian group G is not polynomial, then it is at least $c^{n^{1/d}}$ for some positive integer d (where $c > 1$ is a suitable constant). For each integer $d > 1$ we construct a finitely presented metabelian group whose subgroup growth is approximately $c^{n^{1/d}}$. Finally, we establish a sharp upper bound for the subnormal subgroup growth of finitely presented soluble groups, and derive a new necessary condition for a metabelian group to be finitely presented. Our methods involve results from algebraic geometry and the geometry of numbers, as well as Golod–Safarevic type inequalities.

1. Introduction

We denote by $s_n(G)$ the number of subgroups of index at most n in a group G . The group G is said to have polynomial subgroup growth (PSG) if $s_n(G)$ is bounded above by some fixed power of n ; the study of such groups, begun in [12], has culminated in the recent proof that a finitely generated residually finite group G has PSG if and only if G is virtually soluble of finite rank [8; 5, Chapter 6].

What can be said about the growth rate of $s_n(G)$ if this is faster than polynomial? A recent work of Lubotzky [7] shows that semisimple arithmetic groups G with the congruence subgroup property satisfy

Correspondence to: Dr D. Segal, All Souls College, Oxford OX1 4AL, United Kingdom.

$$s_n(G) \sim n^{\log n / \log \log n}.$$

Thus it is possible for $s_n(G)$ to grow only slightly faster than a polynomial in n . If we stick to nice classes of soluble groups, however, there is a big jump between PSG and non-PSG: in particular we shall see that for a finitely generated nilpotent-by-abelian-by-finite group G , either G has PSG or (for all large n)

$$s_n(G) \geq c^{n^\gamma}$$

for some constants $c > 1$ and $0 < \gamma \leq 1$. Thus for soluble linear groups, for example, the subgroup growth is either at most polynomial, or at least ‘fractionally exponential’. This is a corollary of Theorem 1.1, which deals with metabelian groups. We denote by $s_n^{\triangleleft\triangleleft}(G)$ the number of subnormal subgroups of index at most n in a group G .

Theorem 1.1. *Let G be a finitely generated metabelian group of infinite rank. Then for some constant $c > 1$ we have*

$$s_n(G) \geq s_n^{\triangleleft\triangleleft}(G) \geq c^{n^{1/d}} \quad \text{for all large } n,$$

where d is the Hirsch length of G^{ab} .

The same result is valid for pro- p groups. It shows that the gap between PSG and non-PSG in metabelian pro- p groups is much larger than the gap in arbitrary pro- p groups. Indeed, the minimal subgroup growth of a non-PSG pro- p group is approximately $n^{\log n}$, as shown in [13]; see also [9] for more general constructions of pro- p groups with intermediate subgroup growth.

As regards upper bounds, Mann has recently shown that the subgroup growth of any finitely generated soluble (or indeed pro-soluble) group is at most exponential [10]. Our next theorem shows that there are groups for which this growth is fractionally exponential, with arbitrarily small fractional exponent.

Theorem 1.2. *For each integer $d > 1$ there exist a finitely presented metabelian group G and constants $b, c > 1$ such that*

$$b^{n^{1/d}} \leq s_n^{\triangleleft\triangleleft}(G) \leq s_n(G) \leq c^{n^{1/d}} \quad \text{for all large } n.$$

In our construction G^{ab} has Hirsch length exactly d , so the lower bound on $s_n^{\triangleleft\triangleleft}$ follows from Theorem 1.1. The analogue for $d = 1$ of the above result is immediate from Mann’s theorem; an easy example is provided by $C_p \wr C_\infty$. As we shall see, such examples cannot be finitely presented.

To the best of our knowledge, Theorem 1.2 provides the first examples of groups with fractionally exponential subgroup growth; for analogous phenomena

of groups with intermediate word growth, see [6]. As may be expected, our analysis of metabelian groups involves some commutative algebra. However, while the results needed in the proof of Theorem 1.1 are fairly elementary, obtaining the upper bound in Theorem 1.2 seems to require somewhat deeper tools. The proof we give relies on a version of Bézout's Theorem in algebraic geometry, as well as on Minkowski's fundamental theorem in the geometry of numbers.

The finitely presented metabelian groups that we construct for Theorem 1.2 have periodic derived groups. Our third main result gives a general upper bound for the subnormal subgroup growth of groups in this class.

Theorem 1.3. *Let G be a finitely presented group having a periodic abelian normal subgroup A such that G/A is nilpotent. Then there exists $c \geq 1$ such that*

$$s_n^{\triangleleft\triangleleft}(G) \leq c^{n^{1/2}} \quad \text{for all } n.$$

Combined with Theorem 1.1, this provides a large class of groups whose subnormal subgroup growth is 'semi-exponential' in a fairly precise sense:

Corollary 1.4. *Let G be a finitely presented metabelian group of infinite rank, such that G' is periodic and $h(G/G') = 2$. Then*

$$\lim_{n \rightarrow \infty} (\log \log s_n^{\triangleleft\triangleleft}(G) / \log n) = 1/2.$$

Our last main theorem is more general, with a slightly weaker conclusion:

Theorem 1.5. *Let G be a finitely presented soluble group. Then there exists $g > 0$ such that*

$$s_n^{\triangleleft\triangleleft}(G) \leq n^{gn^{1/2}} \quad \text{for all } n.$$

For comparison with the other results, we note the following immediate corollary:

Corollary 1.6. *Let G be a finitely presented soluble group. Then for each $\varepsilon > 0$ there exists $c = c(\varepsilon) > 0$ such that*

$$s_n^{\triangleleft\triangleleft}(G) \leq c^{n^{1/2+\varepsilon}} \quad \text{for all } n.$$

Combining this with a sharper version of Theorem 1.1 (Theorem 2.2), we shall derive a new and simple necessary condition for a metabelian group to be finitely presentable; its statement, which is somewhat technical, is deferred to Section 6 (see Corollary 6.4). This result is independent of the powerful geometrical

methods of Bieri and Strebel [2]; however, it does depend on a recent deep result of Wilson [14], as do Theorems 1.3 and 1.5.

Notation. Notation is mostly standard. $\text{Dim}(R)$ denotes the Krull dimension of a ring R . The Hirsch length of a group G is denoted by $h(G)$ and $d(G)$ denotes its minimal number of generators. \hat{G} is the profinite completion of G and we set $\hat{d}(G) = d(\hat{G})$. The minimal number of generators of an R -module M is denoted $d_R(M)$. If M is a $\mathbb{Z}G$ -module and H is a subgroup of G , then M_H stands for the restriction of M to H . G^n denotes the subgroup generated by all n th powers in a group G . The centre of G is denoted $Z(G)$, the derived subgroup of G is denoted by G' and we set $G^{\text{ab}} = G/G'$. We write $\log n$ for $\log_2 n$.

2. The lower bound and the invariant γ

Let Γ be a finitely generated abelian group, p a prime, and P a prime ideal of the group ring $\mathbb{F}_p\Gamma$. Write $\Gamma_p = \Gamma \cap (1 + P)$. Now define

$$\gamma(\mathbb{F}_p\Gamma/P) = \text{Dim}(\mathbb{F}_p\Gamma/P) / h(\Gamma/\Gamma_p).$$

Note that this expression is not defined if P is maximal (in which case both numerator and denominator vanish). So let us take γ to be 0 in this case.

If M is a finitely generated $\mathbb{F}_p\Gamma$ -module, define

$$\gamma(M) = \sup\{\gamma(\mathbb{F}_p\Gamma/P_i) \mid i = 1, \dots, s\},$$

where P_1, \dots, P_s are the associated prime ideals of M in $\mathbb{F}_p\Gamma$. Finally, if M is a finitely generated $\mathbb{Z}\Gamma$ -module, set

$$\gamma(M) = \sup\{\gamma(M/pM) \mid p \text{ prime}\}. \quad (1)$$

It is easy to verify the following properties of this invariant, using elementary results from commutative algebra.

- (i) $0 \leq \gamma(M) \leq 1$.
- (ii) $\gamma(M) = 0$ if and only if M has finite rank as a \mathbb{Z} -module; if $\gamma(M) \neq 0$ then $\gamma(M) \geq h(\Gamma)^{-1}$.
- (iii) As p varies over all primes, $\gamma(M/pM)$ takes only finitely many distinct values, so the supremum in (1) is attained; hence $\gamma(M)$ is always rational.
- (iv) If Γ is infinite and M is a finitely generated free $\mathbb{F}_p\Gamma$ -module then $\gamma(M) = 1$.
- (v) Let Δ, Λ be subgroups of Γ such that Δ has finite index and $\Lambda \triangleleft \Gamma$ acts trivially on M ; then $\gamma(M_\Delta) = \gamma(M_\Gamma) = \gamma(M_{\Gamma/\Lambda})$.

Now, let G be a finitely generated metabelian-by-finite group. Then G has

normal subgroups $A \subseteq K$ such that A and K/A are abelian and G/K is finite. Put $\Gamma = K/A$ and define

$$\gamma(G) = \gamma(A_\Gamma) ;$$

it is not hard to check (using (ii) and (v) above) that this is independent of the choices made. Property (ii) also gives rise to the following.

Lemma 2.1. *Let G be a finitely generated metabelian-by-finite group. Then $\gamma(G) = 0$ if and only if G has finite rank. If $\gamma(G) \neq 0$ and G is metabelian, then $\gamma(G) \geq h(G^{\text{ab}})^{-1}$. \square*

We can now formulate the main result of this section.

Theorem 2.2. *Let $G \neq 1$ be a finitely generated metabelian-by-finite group. Put $\gamma = \gamma(G)$. Then there exists $c > 1$ such that $s_n^{\triangleleft \triangleleft}(G) \geq c^{n^\gamma}$ for all large n .*

This result (with the lemma preceding it) implies Theorem 1.1. The claim made in the Introduction about nilpotent-by-abelian-by-finite groups also follows, since if such a group has infinite rank then so also does one of its metabelian-by-finite quotients.

The rest of this section is devoted to the proof of Theorem 2.2.

Let $A \subset K \subseteq G$ be as above, and suppose, without loss of generality, that K/A is free abelian. There exist a prime p and a prime ideal P of $\mathbb{F}_p(K/A)$ such that $\gamma(G) = \gamma(\mathbb{F}_p(K/A)/P)$. The $\mathbb{F}_p(K/A)$ -module A has a quotient module M which is a finitely generated torsion-free $\mathbb{F}_p(K/A)/P$ -module.

Put $\Gamma = K/C_K(M) = (K/A)/(K/A)_P$, and let $d = h(\Gamma)$.

Set $R = \mathbb{F}_p\Gamma/\text{ann}(M) = \mathbb{F}_p\Gamma/\bar{P}$ where \bar{P} is the image of P in $\mathbb{F}_p\Gamma$. Then $\text{Dim}(R) = \text{Dim}(\mathbb{F}_p(K/A)/P) = r$, say, and by definition we have

$$\gamma(G) = r/d .$$

Since the theorem is trivial if $\gamma(G) = 0$ we may assume that $r \geq 1$.

Lemma 2.3. *Let L be a maximal ideal of R and denote by r_L the dimension of the local ring R_L . Then there exists $a > 0$ such that $\dim_{\mathbb{F}_p}(M/ML^n) \geq an^{r_L}$ for all n .*

Proof. The Hilbert–Serre theorem (see [1, Chapter 11]) shows that, for some $b > 0$, $\dim_{\mathbb{F}_p}(R/L^n) \geq bn^{r_L}$ for all large n . Now, M contains a copy of the R -module R . It follows by the Artin–Rees lemma that there exists k such that $\dim_{\mathbb{F}_p}(M/ML^n) \geq \dim_{\mathbb{F}_p}(R/L^{n-k})$ for all $n \geq k$. Taking $0 < a < b$ we obtain the desired inequality for all large n . Now make a smaller if necessary to handle the finitely many remaining inequalities. \square

Now, choose a maximal ideal L of R such that $r_L = r$ (this holds for almost all L), and put $\Delta = \Gamma_L$. Note that Γ/Δ is finite since R/L is a finite ring, and that Δ is torsion-free (Γ has no p -torsion because $\text{char } R = p$, and Γ_L has no p' -torsion because it is residually a p -group, by Krull's intersection theorem). Hence Δ is a free abelian group of rank d . For each m we have (in the ring $\mathbb{F}_p \Gamma$)

$$\Delta^{p^m} - 1 \subseteq (\Delta - 1)^{p^m} \subseteq L^{p^m},$$

and by Lemma 2.3 we see that for all m ,

$$\dim_{\mathbb{F}_p}(M/M(\Delta^{p^m} - 1)) \geq ap^{mr}. \quad (2)$$

Now fix m for the moment and let B be the inverse image of $M(\Delta^{p^m} - 1)$ in A . Write H for the inverse image of Δ^{p^m} in G , and denote by $\bar{}$ the natural map of H onto H/B . Then \bar{A} is an elementary abelian p -group of rank k , say, where $k \geq ap^{mr}$ by (2).

We claim that AH^p has an elementary abelian p -quotient of rank k . To see this, note that $\bar{H}' \subseteq \bar{A} \subseteq Z(\bar{H})$. Since \bar{A} has exponent p this implies that $\bar{H}^p \subseteq Z(\bar{H})$, and hence that $\overline{AH^p}$ is abelian. As every subgroup of a finitely generated abelian group is isomorphic to a suitable factor group, the claim follows.

Now, an elementary abelian p -group of rank k has at least p^{k-1} maximal subgroups. Since $k \geq ap^{mr}$ it follows that AH^p has at least $p^{ap^{mr}-1}$ normal subgroups of index p .

Put $q = |G : K| \cdot |\Gamma : \Delta|$, $s = d(K/A)$. Then $|G : H| = qp^{md}$ since Δ is free abelian of rank d . We also have $|H : AH^p| = p^s$. It follows that G contains at least $p^{ap^{mr}-1}$ subnormal subgroups of index qp^{md+s+1} .

Finally, let n be a large positive integer and choose m such that

$$(qp^{s+1})p^{md} \leq n < (qp^{s+1})p^{(m+1)d}.$$

It follows from the above that, provided n is large enough, G contains at least $c^{n^{r/d}}$ subnormal subgroups of index at most n , where

$$c = p^{a(2qp^{s+d+1})^{-1}} > 1.$$

This establishes Theorem 2.2. Actually, the same argument yields a stronger result: by choosing Δ above to be a G -invariant subgroup of Γ contained in $1 + L$, we could have obtained the same result for 2-step subnormal subgroups of G .

The proof also shows that, for a suitable normal subgroup D of finite index in G , the pro- p completion \hat{D}_p of D satisfies

$$s_n(\hat{D}_p) \geq c^{n^{\gamma(G)}}$$

for all large n .

Finally, if G is assumed to be a (metabelian-by-finite) pro- p group to begin with, then Theorem 2.2 holds for G with a similar (in fact somewhat simpler) proof.

3. The upper bounds: preliminary reductions

The purpose of this section is to reduce the problem of bounding the subgroup growth of certain groups to that of bounding the numbers of generators of a certain module over various subgroups.

If R is a ring and M is an R -module, we define

$$\hat{d}_R(M) = \sup\{d_R(\bar{M}) \mid \bar{M} \text{ is a finite quotient module of } M\},$$

and if $R = \mathbb{Z}G$ for a group G ,

$$\hat{d}_R^n(M) = \sup\{d_R(\bar{M}) \mid \bar{M} \text{ is a finite nilpotent quotient module of } M\}$$

(by a *nilpotent* G -module we mean one on which G acts nilpotently).

Our aim is to establish the following:

Proposition 3.1. *Let G be a group and A an abelian normal subgroup of G which is finitely generated as a G -operator group. Suppose that G/A has finite rank, and that there exist $q > 0$ and $0 < \gamma \leq 1$ such that either (i):*

$$\hat{d}_{\mathbb{Z}K}(A) \leq q \mid G : K \mid^\gamma$$

for every finite index subgroup K of G , or (ii):

$$\hat{d}_{\mathbb{Z}K}^n(A) \leq q \mid G : K \mid^\gamma$$

for every finite index subgroup K of G . Then there exists $c > 1$ such that, in case (i),

$$s_n(G) \leq c^{n^\gamma} \quad \text{for all } n,$$

and in case (ii),

$$s_n^{\triangleleft}(G) \leq c^{n^\gamma} \quad \text{for all } n.$$

In order to prove this result we need the following lemmas.

Lemma 3.2. *Let γ and $m \leq n$ be positive real numbers, and let $c = e^{(e^\gamma)^{-1}}$. Then*

$$(n/m)^{m^\gamma} \leq c^{n^\gamma}.$$

(Here e denotes the base of the natural logarithms.)

Proof. Elementary calculus. \square

Lemma 3.3. *Let G be a group with $d = \hat{d}(G) < \infty$ and let M be a finitely generated $\mathbb{Z}G$ -module. Put $f = \hat{d}_{\mathbb{Z}G}(M) < \infty$ and $g = \hat{d}_{\mathbb{Z}G}^n(M)$. Then, for each n , the number of $\mathbb{Z}G$ -submodules of index at most n in M is at most $n^{f+2+d \log n}$, and the number of $\mathbb{Z}G$ -submodules B of index at most n in M such that G acts nilpotently on M/B is at most $n^{g+2+d \log n}$.*

Proof. Given (the elementary fact) that the number of partitions of a positive integer k is at most 2^{k-1} , it is easy to see that there are no more than n^2 isomorphism types of \mathbb{Z} -modules of order at most n (this crude estimate can of course be significantly improved).

Such a \mathbb{Z} -module N can be generated by at most $\log n$ elements, and thus its automorphism group has order at most $n^{\log n}$. It follows that N can be made into a $\mathbb{Z}G$ -module in at most $(n^{\log n})^d$ ways (note that a finite $\mathbb{Z}G$ -module is a $\mathbb{Z}\hat{G}$ -module).

We conclude that there are at most $n^{2+d \log n}$ isomorphism types of $\mathbb{Z}G$ -modules of order at most n . Let I be the intersection of their annihilators in $\mathbb{Z}G$, and put $\bar{M} = M/MI$. Then \bar{M} is finite; any $\mathbb{Z}G$ -submodule L of index at most n in M gives rise to a homomorphism from \bar{M} onto M/L and L is determined by that homomorphism. Since there are at most n^f $\mathbb{Z}G$ -module homomorphisms from \bar{M} into any given $\mathbb{Z}G$ -module of order at most n , it follows that M has no more than $n^{2+f+d \log n}$ submodules of index at most n .

The second statement of the lemma is proved in exactly the same way. \square

Let us now prove Proposition 3.1. Since G/A has finite rank, r say, we have

$$s_n(G/A) \leq n^\alpha \quad \text{for all } n,$$

where α is a constant depending on r [11, Theorem 3.4]. Fix a subgroup K/A of index $m \leq n$ in G/A . According to our assumptions we have $\hat{d}_{\mathbb{Z}K}(A) \leq qm^\gamma$. By Lemma 3.3 A has at most $k^{2+qm^\gamma+d \log k}$ $\mathbb{Z}K$ -submodules of index k in A , where $k \geq 1$ is any integer. Let B be one of them. Then, since $d(K/A) \leq r$, there are at most k^r complements for A/B in K/B .

Now suppose H is a subgroup of index at most n in G . Putting $K = AH$ and $B = A \cap H$ we see that H/B is a complement for A/B in K/B . If $m = |G : K|$ and $k = n/m$ then $|A : B| \leq k$.

It follows from the preceding discussion that the number of possibilities for H is at most $\sum_{m \leq n} f(n, m)$, where

$$f(n, m) = m^\alpha \cdot (n/m)^{2+qm^\gamma+d \log(n/m)} \cdot (n/m)^r.$$

An elementary manipulation based on Lemma 3.2 shows that, for some constant b , we have $f(n, m) \leq b^{n^\gamma}$ for all n and $m \leq n$. Finally, let $w = \sup_{n \geq 1} n^{n^{-\gamma}}$ (this is finite) and put $c = wb$. Then

$$s_n(G) \leq \sum_{m \leq n} f(n, m) \leq nb^{n^\gamma} \leq c^{n^\gamma}.$$

This completes the proof of case (i).

Case (ii) follows by the same argument, provided we can show that if H , above, is subnormal in G , then the module $A/B = A/A \cap H$ is acted on nilpotently by the group $K = AH$. Suppose H is t -step subnormal in G . Then

$$[A, K, \dots, K] = [A, H, \dots, H] \leq A \cap H = B,$$

where the commutators are repeated t times. Thus K acts nilpotently on A/B as required. \square

4. Good primes and theorems of Bézout and Minkowski

In this section we describe a class of finitely generated metabelian groups G for which the growth rate of $s_n(G)$ can be estimated rather precisely; indeed, for these groups we establish an upper bound on $s_n(G)$ similar to the lower bound provided in Theorem 2.2. The fact that the class of groups we describe is not empty will be established in the next section.

The following notion will play a key role.

Definition. (1) Let Γ be a finitely generated abelian group, p a prime, and P a prime ideal of $\mathbb{F}_p\Gamma$. Write $\bar{}$ for the natural projection $\mathbb{F}_p\Gamma \rightarrow \mathbb{F}_p(\Gamma/\Gamma_p)$. Let $d = h(\bar{\Gamma})$ and $r = \text{Dim}(\mathbb{F}_p\Gamma/P)$. We say that P is *good* if $\bar{\Gamma}$ has a free abelian subgroup $\bar{\Sigma}$ of finite index such that

- (i) $\bar{P} \cap \mathbb{F}_p\bar{\Sigma}$ can be generated by $d - r$ elements as an ideal of $\mathbb{F}_p\bar{\Sigma}$, and
- (ii) whenever Δ is a free abelian subgroup of rank r in $\bar{\Sigma}$ and T is a maximal ideal of $\mathbb{F}_p\Delta$, the ideal $T \cdot \mathbb{F}_p\bar{\Sigma} + \bar{P}$ has finite index in $\mathbb{F}_p\bar{\Sigma}$.

(2) More generally, we call a finitely generated $\mathbb{Z}\Gamma$ -module *good* if for every prime p , each associated prime ideal of M/pM in $\mathbb{F}_p\Gamma$ is good.

(3) Let G be a metabelian group. We say that G is *good* if

- (i) G is finitely generated and has infinite rank;
- (ii) G has an abelian normal subgroup A such that G/A is abelian, and A is a torsion group which is good as a $\mathbb{Z}(G/A)$ -module.

(4) A metabelian-by-finite group is said to be *good* if it has a good metabelian subgroup of finite index.

We now state the main result of this section. For the definition of $\gamma(G)$, see Section 2.

Theorem 4.1. *Let G be a good metabelian-by-finite group. Then there exists $c > 1$ such that $s_n(G) \leq c^{n^{\gamma(G)}}$ for all n .*

The rest of this section is devoted to the proof of this theorem. It clearly suffices to prove the theorem in the metabelian case. First note that, in view of Proposition 3.1, it suffices to establish the following.

Proposition 4.2. *Let G be a good metabelian group, and let $A \triangleleft G$ be as in the definition of goodness. Then there exists $q > 0$ such that*

$$\hat{d}_{\mathbb{Z}K}(A) \leq q |G : K|^{\gamma(G)}$$

for every finite index subgroup K of G .

The proof depends on three preliminary lemmas.

Lemma 4.3. *Let R be a commutative Noetherian ring, M a finitely generated R -module, and P_1, \dots, P_t the associated primes of M . Suppose M has a filtration such that each R/P_i occurs m_i times in its factors. Let S be a finitely generated subring of R . Then, for each i ,*

$$\hat{d}_S(R/P_i) = \sup\{\dim_{S/L}(R/(P_i + RL)) : L \text{ a maximal ideal of } S\},$$

and

$$\hat{d}_S(M) \leq \sum_{i=1}^t m_i \hat{d}_S(R/P_i). \quad \square$$

The proof is elementary and is left to the reader.

The following result relies on Minkowski's fundamental lattice point theorem (or rather on a suitable extension of it). The l_1 -norm of a vector $v = (a_1, \dots, a_d) \in \mathbb{R}^d$ is denoted by

$$|v|_1 = |a_1| + \dots + |a_d|.$$

Lemma 4.4. *Let Λ be a subgroup of finite index n in \mathbb{Z}^d and let $1 \leq r \leq d$. Then there exist r linearly independent vectors $v_1, \dots, v_r \in \Lambda$ such that*

$$|v_1|_1 \cdot \dots \cdot |v_r|_1 \leq c \cdot n^{r/d},$$

where c is a constant depending only on d .

Proof. By [4, Chapter VIII, Theorem I and Lemma 1], there exists a constant $b \geq 1$ (depending on d) such that any lattice of volume n in \mathbb{R}^d has a basis v_1, \dots, v_d satisfying

$$\prod_{i=1}^d |v_i|_2 \leq bn$$

where $|v|_2$ is the l_2 -norm of v . Since $|v|_1 \leq \sqrt{d}|v|_2$ we obtain

$$\prod_{i=1}^d |v_i|_1 \leq cn, \quad (3)$$

where $c = b \cdot d^{d/2}$.

Now, the index of the subgroup $\Lambda \subseteq \mathbb{Z}^d$ coincides with its volume as a lattice, and so the result in the case $r = d$ follows.

In general, let v_1, \dots, v_d form a basis of Λ satisfying (3). Assuming $|v_1|_1 \leq |v_2|_1 \leq \dots \leq |v_d|_1$ as we may, we obtain

$$\prod_{i=1}^r |v_i|_1 \leq (cn)^{r/d} \leq cn^{r/d}$$

as required. \square

The next lemma is a form of Bézout's Theorem in algebraic geometry. As we have been unable to find a suitable reference for the version we need, we sketch a proof for the reader's convenience.

Lemma 4.5. *Let k be a field and $R = k[X_1, \dots, X_m]$ the polynomial ring. Let $f_1, \dots, f_m \in R$ be of (total) degrees e_1, \dots, e_m respectively, and let I be the ideal they generate in R . Suppose $\dim_k(R/I) < \infty$. Then*

$$\dim_k(R/I) \leq e_1 \cdot \dots \cdot e_m.$$

Proof. Since I has finite codimension in R , the sequence $\{f_i\}$ is regular, i.e. each element f_i is not a zero divisor modulo the ideal generated by its predecessors. Now, suppose first that the polynomials are homogeneous, and set $I_j = (f_1, \dots, f_j)$ for $0 \leq j \leq m$ (where $I_0 = (0)$). Then each $R_j = R/I_j$ is an \mathbb{N} -graded ring, and as such it has a Hilbert–Poincaré function $F_j(z) = \sum_{n \geq 0} a_n(j) z^n$ where $a_n(j)$ is the dimension of the n th homogeneous component of R_j . Clearly

$$F_0(z) = (1 - z)^{-m}.$$

Since f_1 is homogeneous of degree e_1 and is not a zero divisor in $R_0 = R$ we have

$$F_1(z) = F_0(z)(1 - z^{e_1}) = (1 - z)^{-m}(1 - z^{e_1}).$$

Proceeding in this manner we obtain

$$F_m(z) = (1-z)^{-m} \prod_{j=1}^m (1-z^{e_j}) = \prod_{j=1}^m (1+z+z^2+\cdots+z^{e_j-1}).$$

This function has no poles at $z=1$ and substituting $z=1$ in it we get

$$\dim_k(R_m) = \sum_{n \geq 0} a_n(m) = F_m(1) = \prod_{j=1}^m e_j$$

which proves the claim.

The proof for non-homogeneous polynomials is obtained by a standard homogenisation process and is left to the reader. \square

The main step in proving Proposition 4.2 is the following:

Lemma 4.6. *Let Γ be a finitely generated abelian group, p a prime, and P a good prime ideal of $\mathbb{F}_p \Gamma$. Then there exists $q > 0$ such that for each finite index subgroup $\Lambda \subseteq \Gamma$ and each maximal ideal L of $\mathbb{F}_p \Lambda$ we have*

$$\dim_{\mathbb{F}_p \Lambda / L}(\mathbb{F}_p \Gamma / (P + L \cdot \mathbb{F}_p \Gamma)) \leq q \cdot |\Gamma : \Lambda|^{r/d},$$

where $d = h(\Gamma / \Gamma_p)$ and $r = \text{Dim}(\mathbb{F}_p \Gamma / P)$.

Proof. We may assume (to simplify notation) that $\Gamma_p = 1$. Let $\Sigma = \langle x_1, \dots, x_d \rangle$ be the subgroup of Γ specified in the definition of good prime ideals. Let Λ be a subgroup of finite index in Γ and let L be a maximal ideal of $\mathbb{F}_p \Lambda$. Put $\Lambda_0 = \Lambda \cap \Sigma$. Then $|\Sigma : \Lambda_0| \leq |\Gamma : \Lambda|$, and $L_0 = L \cap \mathbb{F}_p \Lambda_0$ is a maximal ideal of $\mathbb{F}_p \Lambda_0$ (as $\mathbb{F}_p \Lambda / L$ is a finite field).

Moreover, it is easy to see that

$$\begin{aligned} \dim_{\mathbb{F}_p \Lambda / L}(\mathbb{F}_p \Gamma / (P + L \mathbb{F}_p \Gamma)) \\ \leq |\Gamma : \Sigma| \cdot \dim_{\mathbb{F}_p \Lambda_0 / L_0}(\mathbb{F}_p \Sigma / (P \cap \mathbb{F}_p \Sigma + L_0 \mathbb{F}_p \Sigma)). \end{aligned}$$

We may therefore simplify notation further and replace Γ by Σ and P by $P \cap \mathbb{F}_p \Sigma$; note that d, r remain unchanged in this process.

So let Λ be a subgroup of finite index n in Σ and let L be a maximal ideal of $\mathbb{F}_p \Lambda$. We have to show that

$$\dim_{\mathbb{F}_p \Lambda / L}(\mathbb{F}_p \Sigma / (P + L \mathbb{F}_p \Sigma)) \leq q n^{r/d}, \quad (4)$$

where q is independent of Λ, L, n .

The first step is to invoke Lemma 4.4; this shows that Λ contains a free abelian subgroup $\Delta = \langle h_1, \dots, h_r \rangle$ of rank r , where

$$h_i = \prod_{j=1}^d x_j^{w_{ij}} \quad (1 \leq i \leq r)$$

and

$$\prod_{i=1}^r \sum_{j=1}^d |w_{ij}| \leq cn^{r/d} \quad (5)$$

(here c depends on d only).

Put $T = L \cap \mathbb{F}_p \Delta$ and note that T is a maximal ideal of $\mathbb{F}_p \Delta$. Since P is good, this implies that $S = \mathbb{F}_p \Sigma / (P + T \mathbb{F}_p \Sigma)$ is finite. It also follows that P has a generating set $\{g_{r+1}, \dots, g_d\}$ of size $d - r$.

We may—and do—choose each $g_i = g_i(x_1, \dots, x_d)$ to lie in the subring $\mathbb{F}_p[x_1, \dots, x_d]$ of $\mathbb{F}_p \Sigma$, and denote by e_i the total degree of g_i in x_1, \dots, x_d .

Now put $k = \mathbb{F}_p \Delta / T$, and consider the polynomial ring

$$R = k[X_1, \dots, X_d, Y_1, \dots, Y_d]$$

in $2d$ variables. Assume, for the moment, that $P + T \mathbb{F}_p \Sigma$ is a proper ideal of $\mathbb{F}_p \Sigma$. Its intersection with $\mathbb{F}_p \Delta$ is then equal to T , so we can identify k with the image of $\mathbb{F}_p \Delta$ in S . We thus obtain a ring epimorphism $\theta : R \rightarrow S$ with $X_i \theta = \bar{x}_i$ and $Y_i \theta = \bar{x}_i^{-1}$ for each i , where \bar{x} is the image of x in S .

It is easy to verify that $\ker \theta$ is generated by the elements

$$X_i Y_i - 1 \quad (1 \leq i \leq d), \quad g_i(X_1, \dots, X_d) \quad (r+1 \leq i \leq d)$$

and

$$f_i(X_1, \dots, X_d, Y_1, \dots, Y_d) - \mu_i \quad (1 \leq i \leq r),$$

where for each i , $\mu_i = h_i + T \in \mathbb{F}_p \Delta / T = k$ and

$$f_i = \prod_{\{j: w_{ij} \geq 0\}} X_i^{w_{ij}} \prod_{\{j: w_{ij} < 0\}} Y_i^{-w_{ij}}.$$

Note that $\deg(f_i) = \sum_{j=1}^d |w_{ij}|$ and so

$$\prod_{i=1}^r \deg(f_i) \leq cn^{r/d}$$

by (5). Since $\ker \theta$ is generated by $2d$ elements and has finite index in R (as S is finite), Lemma 4.5 is applicable. It shows that

$$\dim_k(S) = \dim_k(R/\ker \theta) \leq 2^d \prod_{i=r+1}^d e_i \prod_{i=1}^r \deg(f_i)$$

and thus

$$\dim_k(S) \leq qn^{r/d}, \quad (6)$$

where $q = 2^d \cdot \prod_{i=r+1}^d e_i \cdot c$.

This was under the assumption that $P + T\mathbb{F}_p\Sigma$ is a proper ideal of $\mathbb{F}_p\Sigma$; but of course the conclusion stands trivially otherwise, since then $S = 0$.

The desired result (4) now follows from (6), since k is a subfield of $\mathbb{F}_p A/L$ and $\mathbb{F}_p\Sigma/(P + L\mathbb{F}_p\Sigma)$ is a quotient of S . \square

The proof of Proposition 4.2 is now readily completed. Let G and A satisfy the assumptions of the proposition and set $\Gamma = G/A$. Since A is both \mathbb{Z} -torsion and Noetherian as a $\mathbb{Z}\Gamma$ -module, A/pA is non-zero for only finitely many primes p . Let K be a finite index subgroup of G and set $\Lambda = KA/A \subseteq \Gamma$. Then

$$|\Gamma : \Lambda| \leq |G : K|$$

and

$$\hat{d}_{\mathbb{Z}K}(A) \leq \hat{d}_{\mathbb{Z}\Lambda}(A) = \sup\{\hat{d}_{\mathbb{F}_p\Lambda}(A/pA) : p \text{ a prime}\}.$$

Also, by hypothesis, for every prime p each associated prime ideal of A/pA in $\mathbb{F}_p\Gamma$ is good. The result now follows from Lemmas 4.3 and 4.6.

5. The existence problem

In this section we show that the preceding theorem is not vacuous, by proving that for every positive integer d there exists a good metabelian group G satisfying $h(G^{\text{ab}}) = d$ and $\gamma(G) = 1/d$ (and that we can make G finitely presented if $d \geq 2$). This fact, combined with Theorems 1.1 and 4.1, clearly implies Theorem 1.2.

Let Γ be a free abelian group of rank $d \geq 1$, and let p be a prime. A prime ideal P of $R = \mathbb{F}_p\Gamma$ is called *faithful* if $\Gamma_P = 1$. Suppose P is faithful and good, with $\text{Dim}(R/P) = r \geq 1$; and let G be any extension (for example, the semi-direct product) of the Γ -module R/P by Γ . It is clear that then G is a good metabelian group, with $\gamma(G) = r/d$ and $h(G^{\text{ab}}) = d$. Thus our task is reduced to the construction of a good faithful prime P of R such that $\text{Dim}(R/P) = 1$. This turns out to be rather easy, because of the following lemma:

Lemma 5.1. *Let Γ be a free abelian group of rank $d \geq 1$, let p be a prime, and let $R = \mathbb{F}_p\Gamma$. Then every faithful prime ideal of height $d - 1$ in R which is generated by $d - 1$ elements is good.*

Proof. Let P be a prime ideal of the indicated type. We must show that if $1 \neq x \in \Gamma$ and L is a maximal ideal of $\mathbb{F}_p\langle x \rangle$, then $P + LR$ has finite index in R . Since $\mathbb{F}_p\langle x \rangle/L$ is finite, we have $x^m - 1 \in L$ for some $m > 0$. Since P is faithful, $x^m - 1 \notin P$, and so its image is not a zero divisor in R/P (as P is prime). Now, $\text{Dim}(R/P) = 1$ by our assumptions. It follows that $R/(P + (x^m - 1)R)$ is a finitely generated \mathbb{F}_p -algebra of Krull dimension zero, hence a finite ring. The result follows. \square

We now exhibit prime ideals of the type mentioned above. Given $d \geq 1$ let $f_1(x), \dots, f_{d-1}(x)$ be distinct monic irreducible polynomials in $\mathbb{F}_p[x]$, all different from x . Let Γ be the free abelian group on x_1, \dots, x_d and consider the following ideal of $R = \mathbb{F}_p\Gamma$:

$$P = (f_1(x_d) - x_1, f_2(x_d) - x_2, \dots, f_{d-1}(x_d) - x_{d-1}).$$

Then

$$R/P \cong \mathbb{F}_p\langle x \rangle[f_1(x)^{-1}, f_2(x)^{-1}, \dots, f_{d-1}(x)^{-1}]$$

is an integral domain of dimension one. It follows that P is a prime ideal of height $d - 1$ which is generated by $d - 1$ elements.

It remains to show that P is faithful. Suppose otherwise. Then there exist integers e_1, \dots, e_d not all zero such that

$$\prod_{i=1}^d x_i^{e_i} - 1 \in P.$$

Putting $f_d(x) = x$ this translates to the following identity in R/P :

$$\prod_{i=1}^d f_i(x)^{e_i} = 1. \quad (7)$$

Since f_1, \dots, f_d are distinct irreducibles of $\mathbb{F}_p[x]$, equality (7) violates unique factorization in that ring. We conclude that P is faithful, hence good by Lemma 5.1.

The fact that the groups we have constructed are in fact finitely presentable, provided that $d \geq 2$, may be deduced from the celebrated criterion of Bieri and Strebel, [2, Theorem A], with the help of Theorem 2.1 of [3]. These reduce the problem to verifying the following claim: considering $\Gamma = \langle f_1, \dots, f_d \rangle$ as a subgroup of the field $\mathbb{F}_p(x)$, there do not exist a non-zero homomorphism $\theta : \Gamma \rightarrow \mathbb{R}$ and a strictly negative real number λ such that both θ and $\lambda\theta$ can be extended to valuations of the field $\mathbb{F}_p(x)$. We leave this as an exercise for the interested reader (note that it is only necessary to consider the (f_i) -adic valua-

tions, for $i = 1, \dots, d$, and the valuation which assigns to a rational function f/g the value $\deg g - \deg f$).

This completes the proof of Theorem 1.2.

It seems likely that more general constructions of good primes will give rise to more types of fractionally-exponential subgroup growth. We anticipate that for every rational number $\alpha \in (0, 1]$ there exists a metabelian group whose growth is approximately c^{n^α} . We leave this for a later project.

6. Subnormal subgroup growth

We shall say that a group G satisfies the condition $\mathcal{W}(\alpha)$ if there exists $f > 0$ such that

$$d(K^{\text{ab}}) \leq f |G : K|^\alpha$$

for every subgroup K of finite index in G (and we call f the *coefficient*). Our results on finitely presented groups depend on recent work of J.S. Wilson on Golod–Safarevic inequalities; we need a specific corollary of this, which we state as the following theorem:

Theorem 6.1. [14, Corollary B]. *Every finitely presented soluble group satisfies $\mathcal{W}(1/2)$.*

Theorems 1.3 and 1.5, stated in the Introduction, are direct consequences of this together with the two main results of this section:

Theorem 6.2. *Let G be a finitely generated group having a periodic abelian normal subgroup A such that G/A is nilpotent. If G satisfies $\mathcal{W}(\alpha)$, where $0 < \alpha \leq 1$, then there exists $c \geq 1$ such that*

$$s_n^{\triangleleft \triangleleft}(G) \leq c^{n^\alpha} \quad \text{for all } n.$$

Theorem 6.3. *Let G be a soluble group satisfying $\mathcal{W}(\alpha)$, where $0 < \alpha \leq 1$. Then there exists $g > 0$ such that*

$$s_n^{\triangleleft \triangleleft}(G) \leq n^{gn^\alpha} \quad \text{for all } n.$$

Before embarking on the proofs, we note the following:

Corollary 6.4. *If G is a finitely generated metabelian group with $\gamma(G) > 1/2$ then G cannot be finitely presented.*

Here, $\gamma(G)$ denotes the invariant defined in Section 2.

Proof. Put $\gamma = \gamma(G) > 1/2$, and suppose that G is finitely presented. Choose $\varepsilon > 0$ with $1/2 + \varepsilon < \gamma$. Then Corollary 1.6 and Theorem 2.2 provide constants $c_1 > 1$ and c_2 such that

$$c_1^{n^\gamma} \leq s_n^{\triangleleft \triangleleft}(G) \leq c_2^{n^{1/2+\varepsilon}}$$

for all large n . Letting n tend to ∞ yields a contradiction. \square

Note that the finitely presented metabelian groups G constructed in Section 5 have $\gamma(G) = 1/d$. Taking $d = 2$ shows that Corollary 6.4 is a best possible result. Indeed, the inequality $\gamma(G) \leq 1/2$ is the only restriction imposed on $\gamma(G)$ by finite presentability of a metabelian group G . To demonstrate this, suppose given any positive rational number $\gamma = r/d \leq 1/2$. Let $\Gamma = \langle x_1, \dots, x_d \rangle$ be free abelian of rank d , and let G be any extension of the Γ -module $\mathbb{F}_p \Gamma / P$ by Γ , where P is the ideal

$$(x_{r+1} - x_1 + a_1, \dots, x_{2r} - x_r + a_r, x_i - x_{ji} + a_{i-r}; \quad 2r < i \leq d),$$

a_1, \dots, a_{d-r} are distinct non-zero elements of \mathbb{F}_p , and j_{2r+1}, \dots, j_d are arbitrary indices in the range $\{1, \dots, r\}$. It is easy to see that then $\gamma(G) = \gamma$, and the main result of [2] may be used to verify that G is finitely presented.

Now we prove Theorem 6.2. Let G and A be as stated. Then A is a Noetherian G -module, by a theorem of P. Hall [15]. Hence the following lemma will reduce the theorem to case (ii) of Proposition 3.1:

Lemma 6.5. *Let $A \triangleleft G$ be as in Theorem 6.2, and suppose that G satisfies $\mathcal{W}(\alpha)$. Then there exists $q > 0$ such that, whenever K is a subgroup of finite index in G and B is a K -submodule of A such that K acts nilpotently on A/B , we have*

$$d_{\mathbb{Z}K}(A/B) \leq q |G : K|^\alpha$$

Proof. Let π be the finite set of primes involved in the torsion of A , put $h = h(G/A)$, and let G_1/A be a torsion-free nilpotent normal subgroup of finite index m , say, in G/A . Denote the nilpotency class of G_1/A by c .

Now suppose K and B are as above, let $n = |G : K|$ and put $H = AK \cap G_1$. Then H/A is torsion-free, and $|G : H| \leq mn$.

An elementary argument shows that

$$d_{\mathbb{Z}K}(A/B) \leq \max\{d(A/A^p[A, H]) \mid p \in \pi\}. \quad (8)$$

We wish to bound the right-hand side of this. So let us, for the moment, fix $p \in \pi$, and write $\bar{} : H \rightarrow H/A_p[A, H]$ for the natural map. Since \bar{H} is nilpotent of class at most $c + 1$, each element of $\bar{H}^{p^{c+1}}$ is the p th power of an element of \bar{H} (see [16, Chapter 6, Proposition 1]). As \bar{H}/\bar{A} is torsion-free and \bar{A} has exponent p , this

implies that $\bar{H}^{p^{c+1}} \cap \bar{A} = 1$. Thus putting $L = A^p[A, H] \cdot H^{p^{c+1}}$ we have $A/A^p[A, H] \cong AL/L$, and so

$$d(A/A^p[A, H]) \leq d((AL)^{\text{ab}}) \leq f|G : AL|^\alpha,$$

where f is the coefficient of $\mathcal{W}(\alpha)$. Now $|H : AL| \leq p^{(c+1)h}$, so $|G : AL| \leq p^{(c+1)h}mn$ and we conclude:

$$d(A/A^p[A, H]) \leq fp^{(c+1)h\alpha} m^\alpha n^\alpha. \quad (9)$$

The lemma now follows from (8) and (9), on putting

$$q = f \cdot \max\{p^{(c+1)h\alpha} : p \in \pi\} \cdot m^\alpha. \quad \square$$

Finally, we give the rather easy counting argument which is the

Proof of Theorem 6.3. Let G be a soluble group of derived length l , satisfying $\mathcal{W}(\alpha)$ with coefficient f . Put $q = c^{2+f}$ where $c = e^{(e\alpha)^{-1}}$ (as in Lemma 3.2). We shall prove that for each n and t , the number $s_n^{(t)}$ of t -step subnormal subgroups of index at most n in G satisfies

$$s_n^{(t)} \leq q^{ln^\alpha}. \quad (10)$$

If K is subnormal of index at most n in G , then is t -step subnormal with $t \leq \log n$; thus (10) implies

$$s_n^{\triangleleft\triangleleft}(G) \leq q^{l \cdot \log n \cdot n^\alpha} = n^{gn^\alpha}$$

where $g = l \cdot \log q$. Thus the theorem will follow once (10) is proved.

To prove (10) we argue by induction on l . Let A be the $(l-1)$ th term of the derived series of G . Let $H/A \leq G/A$, and consider subnormal chains

$$H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_t = K \quad (11)$$

such that $AK = H$ and $|G : K| \leq n$.

Fix $i \leq t$ for the moment, and put $|G : H_{i-1}| = m$. The condition $\mathcal{W}(\alpha)$ gives $d(H_{i-1}^{\text{ab}}) \leq fm^\alpha$. It follows (from Lemma 3.3 for example) that H_{i-1}^{ab} has at most $(n/m)^{2+fm^\alpha}$ subgroups of index at most n/m , and a simple application of Lemma 3.2 shows that this number is no more than q^{n^α} . Now if H_i occurs below H_{i-1} in (11), then $|H_{i-1} : H_i| \leq n/m$, and $H_{i-1}' \leq H_i \leq H_{i-1}$ since $H_{i-1} = H_i(H_{i-1} \cap A)$. Hence there are at most q^{n^α} possible choices for H_i once H_{i-1} is given.

We conclude that, once H is given, the number of possibilities for K is at most q^{ln^α} . Now if K is any t -step subnormal subgroup in G , then K occurs at the bottom

of a chain (11), where $H/A = AK/A$ is t -step subnormal in G/A . By inductive hypothesis, we may suppose that G/A has at most $q^{(t-1)n^a}$ t -step subnormal subgroups of index at most n . Thus (10) follows. \square

References

- [1] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra* (Addison-Wesley, Reading, MA, 1969).
- [2] R. Bieri and R. Strebel, Valuations and finitely presented metabelian groups, *Proc. London Math. Soc.* (3) 41 (1980) 439–464.
- [3] R. Bieri and R. Strebel, A geometric invariant for modules over an Abelian group, *J. Reine Angew. Math.* 322 (1981) 170–189.
- [4] J.W.S. Cassels, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1959).
- [5] J. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic pro- p groups*, London Mathematical Society Lecture Note Series, Vol. 157 (Cambridge University Press, Cambridge, 1991).
- [6] R.I. Grigorchuk, The growth of p -groups and torsion-free groups, *Math. USSR-Sb.* 54 (1986) 185–205.
- [7] A. Lubotzky, Subgroup growth and congruence subgroups, in preparation.
- [8] A. Lubotzky, A. Mann and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.*, to appear.
- [9] A. Lubotzky and A. Shalev, A -analytic pro- p groups, Preprint.
- [10] A. Mann, Positively finitely generated groups, Preprint.
- [11] A. Mann and D. Segal, Uniform finiteness conditions in residually finite groups, *Proc. London Math. Soc.* (3) 61 (1990) 529–545.
- [12] D. Segal, Subgroups of finite index in soluble groups I, in: *Groups—St Andrews 1985*, London Mathematical Society Lecture Note Series, Vol. 121 (Cambridge University Press, Cambridge, 1986) 307–314.
- [13] A. Shalev, Growth functions, p -adic analytic groups, and groups of finite coclass, *J. London Math. Soc.*, to appear.
- [14] J.S. Wilson, Finite presentations of pro- p groups and discrete groups, *Invent. Math.* 105 (1991) 177–183.
- [15] P. Hall, Finiteness conditions for soluble groups, *Proc. London Math. Soc.* (3) 4 (1954) 419–436.
- [16] D. Segal, *Polycyclic Groups* (Cambridge University Press, Cambridge, 1983).